

Sequential Implementation of Global Quantum Operations

L. Lamata,^{1,2} J. León,² D. Pérez-García,³ D. Salgado,⁴ and E. Solano⁵

¹Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, 85748 Garching, Germany

²Instituto de Física Fundamental, CSIC, Serrano 113-bis, 28006 Madrid, Spain

³Dpto. Análisis Matemático, Universidad Complutense de Madrid, 28040 Madrid, Spain

⁴Dpto. Ingeniería Informática, Universidad Antonio de Nebrija, Pirineos 55, 28040 Madrid, Spain

⁵Departamento de Química Física, Universidad del País Vasco-Euskal Herriko Unibertsitatea, Apdo. 644, 48080 Bilbao, Spain

(Received 3 June 2008; published 31 October 2008)

We study the possibility for a global unitary applied on an arbitrary number of qubits to be decomposed in a *sequential* unitary procedure, where an ancillary system is allowed to interact only once with each qubit. We prove that sequential unitary decompositions are in general impossible for genuine entangling operations, even with an infinite-dimensional ancilla, being the controlled-NOT gate a paradigmatic example. Nevertheless, we find particular nontrivial operations in quantum information that can be performed in a sequential unitary manner, as is the case of quantum error correction and quantum cloning.

DOI: 10.1103/PhysRevLett.101.180506

PACS numbers: 03.67.Lx, 03.65.Ta, 42.50.Dv

Unitary evolution, a fundamental pillar of quantum dynamics, can be described as the action of a time-dependent unitary operator on an initial quantum state. In quantum information, the resulting evolution of a global quantum operation acting on N qubits can be rewritten as a quantum circuit made out of one- and two-qubit gates. The application of these gates is nonsequential in general, and the same qubits can be operated repeatedly at different stages of the prescribed quantum algorithm [1]. An arbitrary global unitary is able to produce a unitary transformation that maps N qubits to N qubits. In cases where M of the initial N qubits are unknown and the rest are blanks, as happens in quantum cloning [2] and quantum error correction protocols [3], an $M \rightarrow N$ qubit map that is formally described by an isometric operation can be considered. An isometry is a unitary operation acting only on a subset of its domain.

Engineering a realistic arbitrary global unitary U acting simultaneously on N qubits is known to be a difficult problem. It may be then desirable to decompose U into a sequential unitary procedure, where each qubit is allowed to interact locally and only once with an itinerant ancillary system A , and without measurements (see Fig. 1). The picture of a sequential quantum factory where a global U is decomposed into a sequence of local qubit-ancilla unitary steps is a valid one and could be related to particular quantum Turing machines [4]. However, one should be careful to differentiate this distinct physical problem with the already studied sequential quantum factory of states [5,6]. The latter was shown to be always possible for *any* state, as long as the dimension of the ancilla matches the bond dimension of its corresponding matrix product state (MPS) representation [7]. It is noteworthy to mention the unexpected connection to MPS theory, which has recently shown its power for understanding spin-chain correlations [8], classical simulation of quantum entangled systems [9], and density-matrix renormalization group techniques [10].

In general, sequentiality and the absence of measurements may reduce enormously the complexity in the physical implementation of a global unitary, though they are not unavoidable requirements. However, different experiments and physical settings demand or are restricted to sequential operations for achieving specific quantum information tasks, and allowing measurements may lower the quality of deterministic protocols. Paradigmatic examples are the sequential generation of multiqubit photonic chains, entangled in energy or polarization states [6,11], and the sequential generation of electron-spin entangled states in quantum dot setups [12]. In the former example, the ancillary system can be a cavity mode, while in the latter, it can be a mixed nuclear spin bath. We point out that our proposal is related to the *quantum interface* problem [11], studying the faithful transfer of information from one quantum node to another. From the point of view of unitary operations, Delgado *et al.* [13] proposed recently a sequential implementation of quantum cloning from 1 to N copies, but in their scheme qubit measurements were al-

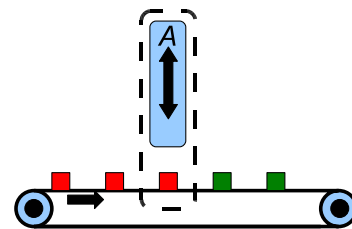


FIG. 1 (color online). Sketch of the proposed sequential quantum factory of operations. When possible, it decomposes a global unitary operation U acting on N qubits into a sequence of local unitary steps where each qubit interacts only once with the ancilla A , and measurements are not allowed. When each qubit-ancilla interaction is finished, the corresponding qubit in the chain leaves the operation region, and the following qubit starts its interaction with A .

lowed to achieve the desired goal. The case of one-way quantum computing [14] is special; it is deterministic and sequential, but it is measurement based and requires the generation of a particular initial entangled state. Below, when we refer to a sequential decomposition, we assume that it is a unitary one, unless other specification is given.

Strikingly, we will prove below that a sequential decomposition of a global unitary U acting simultaneously on N qubits is impossible in general, even with an infinite-dimensional ancilla. By using MPS theory, we will also show how to discriminate the global operations that can be decomposed in a sequential manner and, in the affirmative case, provide with the optimal dimension of the ancilla. We will illustrate our findings with the Shor nine qubit code [15] and the optimal $1 \rightarrow N$ cloning machine [2], showing that the optimal dimension needed for the ancilla in both cases is rather small.

We first illustrate this surprising result with such a simple example as the paradigmatic two-qubit controlled-NOT (CNOT) gate, which flips the target qubit whenever the control qubit is in state $|1\rangle$ and leaves it unchanged when the control qubit is in state $|0\rangle$. We consider a CNOT gate, where qubits 1 and 2 are the control and target qubits, respectively, acting on the initial tripartite state $|a\rangle_1|b\rangle_2|c\rangle_a$. The latter element in this tripartite product state represents an ancillary system A with arbitrary dimension D .

If we could decompose the CNOT gate sequentially, we could write

$$\text{CNOT}_{12} \otimes \mathbb{1}_a = U_{2a}U_{1a}.$$

Therefore, the input $|+00\rangle_{12a}$, $|+\rangle$ being $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, would transform into $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}|0\rangle_a$. This implies (looking at the entanglement in the partition $1|2a$) that $U_{1a}|+\rangle$ has to be maximally entangled. However, $|++0\rangle_{12a}$ remains untouched by the CNOT gate, which implies (again looking at the partition $1|2a$) that $U_{1a}|+\rangle$ is a product state, giving the desired contradiction.

We prove now the following generalization

Theorem 1.—No entangling unitary can be implemented in a sequential way.

Let us call n the smallest i for which $U_{ia} \cdots U_{1a} = U_{1\dots i} \otimes U_a$, that is, the smallest step in which the ancilla always decouples from the qubit chain. This number exists since it happens at least in the N -th step. To finish the argument, it is enough to show that $n = 1$. If it were not true, we could group the first $n - 1$ spins and the n -th one and then have $U_{2a}U_{1a} = U_{12} \otimes \mathbb{1}_a$, where U_{1a} entangles 1 and a (by the choice of n). Therefore, assuming without loss of generality that $U_{1a}|00\rangle$ is entangled, we may write

$$0 = \langle 1_a|U_{2a}U_{1a}|0j0\rangle_{12a} = \sum_{i=0}^r |\phi_i\rangle_1 \langle 1_a|U_{2a}|ij\rangle_{a2}, \quad (1)$$

with $r \geq 1$. Since the $|\phi_i\rangle_1$ are linearly independent,

$\langle 1_a|U_{2a}|ij\rangle_{a2} = 0$ for all j and $i = 0, 1$, implying that $\det(U_{2a}) = 0$ and producing the desired contradiction.

It is noteworthy to notice that, in contrast to the previous negative result, one can *always* implement sequentially a $1 \rightarrow N$ isometry as long as the ancilla dimension is large enough, see Fig. 2. The way to see it is straightforward: (i) we apply locally the desired global isometry on qubit 1 and $N - 1$ blank ancilla qubits, (ii) we implement local swap gates between the ancilla qubits and the $N - 1$ blank chain qubits. Clearly, the worst case scenario will require an exponentially large ancilla dimension, but this fact does not invalidate the previous general claim [16].

Therefore, the remaining task is to find the optimal dimension of the ancilla needed to implement a given $1 \rightarrow N$ isometry. The solution to this problem will come via the use of MPS [7] representations of vectors. They can be defined as

$$|\psi\rangle = \sum_{i_1, \dots, i_N} A_{i_N}^{[N]} A_{i_{N-1}}^{[N-1]} \cdots A_{i_2}^{[2]} A_{i_1}^{[1]} |i_1 i_2 \cdots i_N\rangle, \quad (2)$$

where $A_i^{[m]}$ are $D_{m+1} \times D_m$ matrices with $D_1 = D_{N+1} = 1$. We define the MPS *bond dimension* by $D = \max_i D_i$ and it can be shown [7,9] that there exists a canonical form for any MPS that gives the minimal bond dimension. This MPS canonical form is defined by the conditions: (i) $\sum_i A_i^{[m]\dagger} A_i^{[m]} = \mathbb{1}$, (ii) $\sum_i A_i^{[m]} \Lambda^{[m-1]} A_i^{[m]\dagger} = \Lambda^{[m]}$, for all $1 \leq m \leq N$, and (iii) $\Lambda^{[0]} = \Lambda^{[N]} = 1$ with each $\Lambda^{[m]}$ diagonal, positive, full rank, and $\text{tr} \Lambda^{[m]} = 1$. Since it is obtained by performing successive Schmidt decompositions, this canonical form is essentially unique. Moreover, using Theorem 3.1.1' of [17], one can see that all canonical forms are related by the condition

$$\tilde{A}_i^{[m]} = V_m A_i^{[m]} V_{m-1}^\dagger \quad (3)$$

with $V_0 = V_N = 1$ and V_m unitary such that $[V_m, \Lambda_m] = 0$ for all m .

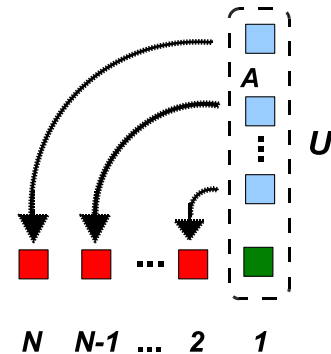


FIG. 2 (color online). Trivial protocol for the sequential decomposition of a $1 \rightarrow N$ isometry. First, the desired isometry is implemented locally between qubit 1 and $N - 1$ qubits in the ancilla degrees of freedom. Second, each ancilla qubit is mapped locally to its corresponding blank chain qubits.

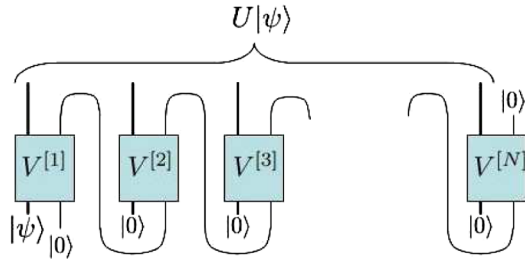


FIG. 3 (color online). Diagram showing the sequential decomposition of a $1 \rightarrow N$ isometry U , acting on an arbitrary initial state $|\psi\rangle$.

In our case, we want to get a canonical MPS representation of the $1 \rightarrow N$ isometry U . We do it by artificially grouping the input and output of the first qubit to get

$$U = \sum_{j_1, i_1, \dots, i_N} A_{i_N}^{[N]} A_{i_{N-1}}^{[N-1]} \dots A_{i_2}^{[2]} A_{i_1, j_1}^{[1]} |i_1\rangle\langle j_1| \otimes |i_2 \dots i_N\rangle. \quad (4)$$

The key observation is to note that the relations

$$\begin{aligned} V^{[1]}|0\rangle_a |j_1\rangle &= \sum_{i_1, k} \langle k | A_{i_1, j_1}^{[1]} |k\rangle_a |i_1\rangle, \\ V^{[k]}|r_k\rangle_a |0\rangle &= \sum_{i_k, s_k} \langle s_k | A_{i_k}^{[k]} |r_k\rangle_a |s_k\rangle_a |i_k\rangle, \end{aligned} \quad (5)$$

allow us to identify the existence of a sequential decomposition of U , as in Fig. 3, with an MPS decomposition of U as in (4) satisfying the additional properties

$$\sum_{i_1} A_{i_1, j_1}^{[1]\dagger} A_{i_1, j'_1}^{[1]} = \delta_{j_1, j'_1}, \quad \sum_i A_i^{[m]\dagger} A_i^{[m]} = \mathbb{1}, \quad m \geq 2. \quad (6)$$

Our main result states that the optimal ancilla to implement U sequentially is exactly the bond dimension of its canonical MPS form. Moreover, any of these canonical MPS representations gives via (5) the sequential decomposition of U as in Fig. 3.

The proof of this result is based on recent mathematical studies in MPS theory [7,9]. We start then with a sequential decomposition of our given $1 \rightarrow N$ isometry, for instance, the one given by Fig. 2. Using (5), this gives an MPS representation for U , using matrices B . We will show that from there, one can obtain a canonical form for U , with matrices A , and still satisfying (6). Using (3), this in turn implies that *all* canonical forms for U satisfy (6).

The procedure to go from matrices B to A was developed in the proof of Theorem 2 in Pérez-García *et al.* [7]. There it is shown how to construct in general nonsquare matrices Z_j with $Z_j^\dagger Z_j = \mathbb{1}$ such that, if we define $A_{i_1, j_1}^{[1]} = Z_1^\dagger B_{i_1, j_1}^{[1]}$, $A_{i_N}^{[N]} = B_{i_N}^{[N]} Z_{N-1}$, and $A_{i_m}^{[m]} = Z_m^\dagger B_{i_m}^{[m]} Z_{m-1}$ for $1 < m < N$, the A 's give a canonical form for the U operator. Moreover, $Z_1 Z_1^\dagger B_{i_1, j_1}^{[1]} = B_{i_1, j_1}^{[1]}$. But we finish now by noticing that

ing that

$$\sum_{i_1} A_{i_1, j_1}^{[1]\dagger} A_{i_1, j'_1}^{[1]} = \sum_{i_1} B_{i_1, j_1}^{[1]\dagger} Z_1^\dagger Z_1 B_{i_1, j'_1}^{[1]} = \delta_{j_1, j'_1}, \quad (7)$$

$$\sum_{i_k} A_{i_k}^{[k]\dagger} A_{i_k}^{[k]} = \mathbb{1}. \quad (8)$$

A useful consequence of the previous result is the following:

Corollary.—If D_i is the optimal bond dimension for $U|i\rangle$, then the optimal ancilla dimension to generate U sequentially is upper bounded by $D_0 + D_1$.

To see it, let us take MPS representations of $U|0\rangle$ and $U|1\rangle$, given by matrices A and B , respectively. Since $U = U|0\rangle\langle 0| + U|1\rangle\langle 1|$, to finish the argument, it is enough to notice that one has the MPS decomposition $U = \sum_{j_1, i_1, \dots, i_N} C_{i_N}^{[N]} \dots C_{i_2}^{[2]} C_{i_1, j_1}^{[1]} |i_1\rangle\langle j_1| \otimes |i_2 \dots i_N\rangle$, taking [18]

$$C^{[N]} = (A_{i_N}^{[N]} |B_{i_N}^{[N]}), \quad C^{[j]} = \begin{pmatrix} A_{i_j}^{[j]} & 0 \\ 0 & B_{i_j}^{[j]} \end{pmatrix}, \quad (9)$$

$$C_{i_1, 0}^{[1]} = \begin{pmatrix} A_{i_1}^{[1]} \\ 0 \end{pmatrix}, \quad C_{i_1, 1}^{[1]} = \begin{pmatrix} 0 \\ B_{i_1}^{[1]} \end{pmatrix}. \quad (10)$$

Let us illustrate the strength of the result with a couple of important examples. The first one is the nine-qubit code of Shor [15], which was the first quantum code that allows to correct an arbitrary one-qubit error. It encodes one qubit into nine, via the encoding map $|0\rangle \mapsto (|000\rangle + |111\rangle)^{\otimes 3}$, $|1\rangle \mapsto (|000\rangle - |111\rangle)^{\otimes 3}$. Since, using the notation of the Corollary, $D_0 = D_1 = 2$, one can implement this encoding operation sequentially with an ancilla consisting of only 2 qubits (dimension 4). This makes the sequential implementation of quantum operations appear as an interesting tool for fault tolerant quantum computation.

The second example is related to optimal quantum cloning [2]. In this context [19], one tries to overcome the restrictions imposed by the no-cloning theorem [20] at the price of lowering the cloning fidelities. In Ref. [21], it is shown how to clone in an optimal way, that is, how to construct a $1 \rightarrow (2N - 1)$ isometry U such that for any of the first N qubits, the clones, one has (i) $\rho_1 = \dots = \rho_N = \rho$ where ρ_i is the reduced density matrix for qubit i of $U|\psi\rangle$ (all clones are equal), (ii) the fidelity $\langle \psi | \rho | \psi \rangle$ between the clones and the original state is maximal. For this U , it is shown in [13] how $D_0 = D_1 = N$. Then, using the Corollary, we conclude that the optimal cloning isometry U of one qubit among N participants can be done sequentially with an ancilla of dimension $2N$, that is, consisting of $\log(N) + 1$ qubits.

We have already demonstrated that in the case of a full $N \rightarrow N$ unitary, no entangling global unitary is decomposable in sequential qubit-ancilla local steps, whereas every $1 \rightarrow N$ isometry has a sequential decomposition. What happens then in the intermediate case of an $M \rightarrow N$ isometry ($M < N$)? As one could expect, there are some non-

trivial (entangling) unitaries that do admit a sequential decomposition. To fully characterize which is the case, one can also apply here the MPS argumentations used in the $1 \rightarrow N$ qubit case to get the following result.

An $M \rightarrow N$ isometry U can be implemented in a sequential manner if and only if $\sum_{i_k} A_{i_k, j_k}^{[k]\dagger} A_{i_k, j'_k}^{[k]} = \delta_{j_k, j'_k} \mathbb{1}$ for

one [and then for all by Eq. (3)] canonical form and for $1 \leq k \leq M$.

As a consequence, if U can be implemented in a sequential manner, the optimal of such decompositions, in terms of the dimension of the ancilla, is given by any of the MPS canonical forms for U , written as

$$U = \sum_{j_1, \dots, j_M, i_1, \dots, i_N} A_{i_N}^{[N]} \dots A_{i_{M+1}}^{[M+1]} A_{i_M, j_M}^{[M]} \dots A_{i_1, j_1}^{[1]} |i_1 \dots i_N\rangle \langle j_1 \dots j_M|. \quad (11)$$

The relations between the sequential decomposition of U as in Fig. 3 and the MPS form (11) are given now by

$$V^{[1]}|0\rangle_a |j_1\rangle = \sum_{i_1, k} \langle k | A_{i_1, j_1}^{[1]} | k \rangle_a | i_1 \rangle,$$

$$V^{[k]}|r_k\rangle_a |j_k\rangle = \sum_{i_k, s_k} \langle s_k | A_{i_k, j_k}^{[k]} | r_k \rangle_a | s_k \rangle_a | i_k \rangle, \quad k \leq M$$

$$V^{[k]}|r_k\rangle_a |0\rangle = \sum_{i_k, s_k} \langle s_k | A_{i_k}^{[k]} | r_k \rangle_a | s_k \rangle_a | i_k \rangle, \quad k > M.$$

In conclusion, we have analyzed the sequential decomposition of arbitrary unitary operations, and we have shown that this is unattainable in general for the $N \rightarrow N$ qubit case. On the other hand, we have proved that the $1 \rightarrow N$ qubit case is always possible, and we have found the optimal ancilla dimension. For the intermediate $M \rightarrow N$ qubit case, with $M < N$, we have given necessary and sufficient conditions for the sequential decomposition to be possible. We believe these results are of importance in the context of quantum theory and quantum information applications. With no doubt, they will prove to be relevant in any future implementation of quantum networks, quantum error correction, quantum cryptographic attacks, and related physical setups.

L.L. is grateful to the Humboldt Foundation for financial support. J.L. and L.L. thank support from Spanish Projects MEC FIS 2005-05304 and CSIC 2004 5 OE 271, and D.P.-G. from MTM2005-00082 and CCG07-UCM/ESP-2797. D.S. acknowledges support from Spanish Ministry of Education Project No. 2008-00288 and E.S. from Ikerbasque Foundation, EU EuroSQIP project, and UPV-EHU Grant GIU07/40.

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

- [2] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, *Rev. Mod. Phys.* **77**, 1225 (2005).
- [3] J. Preskill *Quantum information and computation* edited by H.-K. Lo, S. Popescu, and T.P. Spiller (World Scientific, Singapore, 1998).
- [4] D. Deutsch, *Proc. R. Soc. A* **400**, 97 (1985).
- [5] C. Schön, E. Solano, F. Verstraete, J.I. Cirac, and M.M. Wolf, *Phys. Rev. Lett.* **95**, 110503 (2005).
- [6] C. Schön, K. Hammerer, M.M. Wolf, J.I. Cirac, and E. Solano, *Phys. Rev. A* **75**, 032311 (2007).
- [7] D. Pérez-García, F. Verstraete, M.M. Wolf, and J.I. Cirac, *Quantum Inf. Comput.* **7**, 401 (2007).
- [8] M. Fannes, B. Nachtergaele, and R.F. Werner, *Commun. Math. Phys.* **144**, 443 (1992).
- [9] G. Vidal, *Phys. Rev. Lett.* **91**, 147902 (2003).
- [10] F. Verstraete, D. Porras, and J.I. Cirac, *Phys. Rev. Lett.* **93**, 227205 (2004).
- [11] T. Wilk, S.C. Webster, A. Kuhn, and G. Rempe, *Science* **317**, 488 (2007).
- [12] H. Christ, J.I. Cirac, and G. Giedke, arXiv:0710.4120.
- [13] Y. Delgado, L. Lamata, J. León, D. Salgado, and E. Solano, *Phys. Rev. Lett.* **98**, 150502 (2007).
- [14] R. Raussendorf and H.J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [15] P. Shor, *Phys. Rev. A* **52**, R2493 (1995).
- [16] Note that one could implement any full $N \rightarrow N$ unitary if the following protocol were allowed: (i) we map locally the chain qubits onto blank ancilla qubits, (ii) we apply locally the desired global unitary on the ancilla qubits, (iii) we map *back* locally the ancilla qubits onto their corresponding chain qubits. However, it is clear that this recipe breaks the sequential condition.
- [17] R.A. Horn and C.R. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, Cambridge, 1991).
- [18] We remark that this simple construction only gives directly the canonical MPS form for U in the trivial case $U|0\rangle = |\psi\rangle_{1, \dots, N-1} |\varphi\rangle_N$ and $U|1\rangle = |\phi\rangle_{1, \dots, N-1} |\varphi^\perp\rangle_N$.
- [19] V. Buzek and M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).
- [20] W.K. Wootters and W.H. Zurek, *Nature (London)* **299**, 802 (1982).
- [21] N. Gisin and S. Massar, *Phys. Rev. Lett.* **79**, 2153 (1997).